CCC:MKC
F.# 2020R00563

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
– X

IN THE MATTER OF AN APPLICATION FOR SEARCH WARRANTS FOR:

THE PREMISES KNOWN AND DESCRIBED AS:

ONE GRAY LG PHONE WITH IMEI NUMBER 358335102826284 ("SUBJECT DEVICE 1");

ONE GRAY LG PHONE WITH IMEI NUMBER 354790111345953 ("SUBJECT DEVICE 2");

ONE BLACK IPHONE WITH A WHITE "HOME BUTTON" ("SUBJECT DEVICE 3");

ONE GRAY IPHONE S WITH MODEL NUMBER A1688 AND FCC ID: BCG-E2946A ("SUBJECT DEVICE 4");

ONE BLUE IPHONE IN A CLEAR CASE ("SUBJECT DEVICE 5");

ONE BLACK LG PHONE WITH IMEI NUMBER 356593097595361 AND MODEL NUMBER LML211BL ("SUBJECT DEVICE 6");

ONE GRAY APPLE LAPTOP MODEL NUMBER A1706 AND SN C02TL189GTFJ ("SUBJECT DEVICE 7") (Collectively, the "SUBJECT DEVICES")
– X

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

(Fed. R. Crim. P. 41)

20-MJ-1121

EASTERN DISTRICT OF NEW YORK, SS:

DEREK J. WONDERLAND, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to

law and acting as such. Upon information and belief, there is probable cause to believe that there is located in the PREMISES KNOWN AND DESCRIBED AS: ONE GRAY LG PHONE WITH IMEI NUMBER 358335102826284 ("SUBJECT DEVICE 1"); ONE GRAY LG PHONE WITH IMEI NUMBER 354790111345953 ("SUBJECT DEVICE 2"); ONE BLACK IPHONE WITH A WHITE "HOME BUTTON" ("SUBJECT DEVICE 3"); ONE GRAY IPHONE S WITH MODEL NUMBER A1688 AND FCC ID: BCG-E2946A ("SUBJECT DEVICE 4"); ONE BLUE IPHONE IN A CLEAR CASE ("SUBJECT DEVICE 5"); ONE BLACK LG PHONE WITH IMEI NUMBER 356593097595361 AND MODEL NUMBER LML211BL ("SUBJECT DEVICE 6"); ONE GRAY APPLE LAPTOP MODEL NUMBER A1706 AND SN C02TL189GTFJ ("SUBJECT DEVICE 7") (Collectively, the "SUBJECT DEVICES"), further described in Attachments A-G, for the things described in Attachments H-N, which constitute evidence, fruits and instrumentalities of a narcotics trafficking and narcotics trafficking conspiracy, in violation of Title 21, United States Code, Sections 846 and 841(a)(1), using a firearm in connection with that drug trafficking crime, in violation of Title 18, United States Code, Section 924(c), and illegally possessing a firearm and ammunition having previously been convicted of a felony, in violation of Title 18, United States Code, Section 922(g) (the "SUBJECT OFFENSES").

The source of your deponent's information and the grounds for his belief are as follows:[1]

INTRODUCTION

[1] Because this affidavit is submitted for the limited purpose of establishing probable cause for the search warrants, I have not set forth each and every fact learned during the course of the investigation.

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since 2012. During my tenure with law enforcement, I have participated in numerous investigations involving the illegal sales of narcotics and use of firearms and have conducted or participated in surveillances, the execution of search warrants, debriefings of informants and reviews of taped conversations and telephone records. Through my training, education and experience, I have become familiar with the manner in which narcotics traffickers use cellular telephones to carry out their criminal activities.

2. The facts in this affidavit come from: my personal observations, information provided by Suffolk County Police Department ("SCPD") detectives, a confidential informant (the "CI"),[2] my training and experience, my review of documents, and information obtained from other agents and witnesses.

3. Based on the facts set forth in this affidavit, there is probable cause to believe that GARY JOHNSON, also known as "G-Money," has committed the SUBJECT OFFENSES. There is also probable cause to conclude that the SUBJECT DEVICES are instrumentalities of those offenses and thus to search the SUBJECT DEVICES for evidence, of these crimes as further described in Attachments H-N.

PROBABLE CAUSE

---

2 The CI has been cooperating with federal agents and the SCPD for approximately six months. The CI has proven to be reliable in that information provided by him/her has been corroborated by other sources, including a review of cellular telephone communications, audio and video recordings and text messages, and information provided by other cooperating witnesses. In exchange for the information provided by the CI, he/she has received monetary compensation and has had various vehicle and traffic fines "cleared" from his/her driving record without payment.

4. The FBI and the SCPD have been conducting a criminal investigation of JOHNSON for violations of the SUBJECT OFFENSES. On or about November 18, 2020, a grand jury sitting in the Eastern District of New York returned an indictment charging the defendant with violations of certain of the SUBJECT OFFENSES. Specifically, the defendant was charged with a conspiracy to distribute heroin and fentanyl between January 2015 and October 2020 and sixteen narcotics sales between March 2020 and October 2020. Also on November 18, 2020, the Honorable Anne Y. Shields, United States Magistrate Judge for the Eastern District of New York, signed a warrant authorizing JOHNSON's arrest. That same date, the Honorable Arlene R. Lindsay, United States Magistrate Judge for the Eastern District of New York, signed a warrant authorizing the search of JOHNSON's home (20-MJ-1108).

5. On or about November 19, 2020, law enforcement officers arrested JOHNSON pursuant to that arrest warrant and also searched JOHNSON's home pursuant to the search warrant. During that search and arrest, law enforcement officers recovered the SUBJECT DEVICES from JOHNSON's home. Specifically, the SUBJECT DEVICES were found in the bedroom utilized by JOHNSON, where his personal items were stored, including identification documents and clothing that he asked law enforcement officers to allow him to retrieve on the day of his arrest. Additionally, law enforcement officers recovered a loaded 9mm firearm in a backpack found in the defendant's bedroom; ammunition found in the basement of the home; and drug paraphernalia, including a scale, baggies, press and sifter found in the defendant's bedroom. I reviewed JOHSON's criminal history, which revealed

that he sustained two felony convictions: on February 20, 2007 conviction for Criminal Possession of a Controlled Substance ("CPCS") in the fifth degree in violation of New York Penal Law 220.06(1); and on August 25, 2004, JOHNSON was convicted of Attempted CPCS in the Third Degree in violation New York Penal Law 220.16(1).

6. During the course of its investigation, law enforcement officers have utilized the CI. Between March 2020 and November 2020, the CI, acting at the direction of law enforcement, purchased narcotics from JOHNSON on at least sixteen occasions. On each occasion, the CI communicated with JOHNSON via a cellular telephone for the purpose of scheduling the meeting and confirming the quantity of narcotics the CI sought to purchase from JOHNSON. Moreover, between March 2020 and November 2020 alone, JOHNSON contacted the CI to advise him/her that he was switching to a new cellular telephone number on at least five occasions, thus confirming that JOHNSON has used multiple cellular telephones in furtherance of his crimes. Certain of the narcotics transactions between the CI and JOHNSON are discussed below.

7. On or about March 3, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the cellular telephone number 631-877-3136 (the "3136 Number") for the purpose of arranging a narcotics transaction. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $200. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The Suffolk County Crime Laboratory ("SCCL") subsequently tested

the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of fentanyl.

8. On or about March 5, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 3136 Number for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $600. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of fentanyl.

9. On or about March 11, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the cellular telephone number 631-640-3811 (the "3811 Number") for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $400. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of fentanyl.

10. On or about March 13, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 3811 Number for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $400. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of fentanyl.

11. On or about May 6, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the cellular telephone number 631-644-9044 (the "9044 Number") for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $300. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of fentanyl.

12. On or about May 8, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 9044 Number for

the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $500. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of fentanyl.

13. On or about May 12, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 9044 Number for the purpose of arranging a narcotics transaction. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $600. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of fentanyl.

14. On or about May 20, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 9044 Number for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON.

During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $600. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of heroin and fentanyl.

15. On or about June 12, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 9044 Number for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $200. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of heroin and fentanyl.

16. On or about June 16, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 9044 Number for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $400. JOHNSON and the CI then parted ways. This narcotics transaction was recorded

using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of heroin and fentanyl.

17. On or about July 9, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the cellular telephone number 332-200-3061 (the "3061 Number") for the purpose of arranging a narcotics transaction. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $300. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of heroin.

18. On or about July 29, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 3061 Number for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $300. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown

powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of heroin.

19. On or about August 7, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 3061 Number for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $600. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of fentanyl.

20. On or about August 25, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 3061 Number for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $600. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of heroin and fentanyl.

21. On or about October 14, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the cellular telephone number 631-906-1623 (the "1623 Number") for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $300. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of heroin and fentanyl.

22. On or about October 29, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 1623 Number for the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $300. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The SCCL subsequently tested the brown powdery substance that JOHNSON sold to the CI and confirmed that the substance tested positive for the presence of fentanyl.

23. On or about November 12, 2020, the CI, acting at the direction of law enforcement, communicated with JOHNSON by calling and/or texting the 1623 Number for

the purpose of arranging a narcotics transaction. In those communications, JOHNSON answered the CI via text message. Thereafter, the CI met JOHNSON in a predetermined location in Shirley, New York for the purpose of purchasing narcotics from JOHNSON. During the meeting, JOHNSON handed the CI a brown powdery substance in exchange for $300. JOHNSON and the CI then parted ways. This narcotics transaction was recorded using audio and video recording equipment. The brown powdery substance that JOHNSON sold to the CI field-tested positive for the presence fentanyl.

24. Additionally, after law enforcement recovered the SUBJECT DEVICES, law enforcement placed a call to the 1623 Number the CI used to communicate with JOHNSON, and SUBJECT DEVICE 6 rang, confirming that SUBJECT DEVICE 6 was the same phone used by the CI to communicate with JOHNSON regarding narcotics transactions on October 14, October 29, 2020 and November 12, 2020.

25. Based on my training and experience, I am familiar with the typical distribution and trafficking methods used by drug dealers and traffickers, including the manufacture and distribution of narcotics.

26. In a substantial number of drug investigations, the following kinds of drug-related evidence have typically been recovered:

a. Members of drug organizations often maintain close at hand the addresses and telephone numbers of their criminal associates, including information pertaining to their sources of supply and customers, in mobile telephones.

b. Records of calls to telephones (landlines and mobile telephones). Such records constitute important corroborative evidence in drug conspiracy

cases because the defendants call one another regularly, especially just before and after an incident involving an act committed in furtherance of the conspiracy.

c. Drug traffickers frequently maintain records, receipts, notes, ledgers, and other electronic documents relating to the ordering, sale and distribution of drugs. Such records are generally maintained where the traffickers have ready access to them, such as the trafficker's cellular telephones. Such records are maintained in digital format on cellular phones or other devices that are capable of holding digital data, including laptops.

d. Drug traffickers frequently maintain financial records evidencing the deposit and transfer of monies in their homes. Such records are generally maintained where the traffickers have ready access to them, such as the trafficker's cellular telephones. Such records are maintained in digital format on cellular phones, which are capable of holding digital data or other devices that are capable of holding digital data, including laptops.

e. Based upon my training and experience, as well as my discussions with other law enforcement officers, I am aware that it is generally a common practice for drug traffickers to maintain records relating to their drug trafficking activities. Because drug traffickers will "front" (that is, sell on consignment) controlled substances to their clients, or alternatively, will be "fronted" controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances. Often drug traffickers keep "pay and owe" records to show balances due for drugs sold in the past

("pay") and for payments expected ("owe") as to the trafficker's supplier and the trafficker's dealer(s). Additionally, drug traffickers must maintain telephone and address listings of clients and suppliers and keep them immediately available in order to efficiently conduct their trafficking business. Such records are maintained in digital format and are capable of being stored both on cellular telephones and laptop computers, which are capable of holding digital data.

27. Also, I know, from both my professional and personal experiences, that people often maintain multiple cellular telephones and other cellular telephones capable of holding digital data used to facilitate drug activities. In the instant case, it is clear that JOHNSON utilized at least five different phone numbers throughout the course of the investigation. It is thus unsurprising that six cellular devices were found in his home at the time of his arrest.

28. Based on my training and experience and discussions with other law enforcement officers, I understand that individuals involved in the distribution and possession with intent to distribute narcotics, often do not act alone and often communicate with co-conspirators by means of cellular telephones and laptop computers such as the SUBJECT DEVICES. Such persons commonly maintain records that reflect names, addresses, or telephone numbers of their associates in their cellular telephones. They also commonly maintain records of communications such as call logs, chats and text messages in their cellular telephones. They commonly take photographs of themselves, their associates, or their property using their cellular telephones. These individuals usually maintain these

records of communication and photographs in their possession and in their cellular telephones or other devices capable of storing digital content, such as laptop computers.

29. Each of the SUBJECT DEVICES were found in in close proximity to each other in JOHNSON's bedroom. Specifically, they were located either on the nightstand or JOHNSON's bed. Moreover, the CI has confirmed that he knows JOHNSON to make use of multiple cellular devices and described an occasion when he was at JOHNSON's residence in approximately early Spring 2020 and observed JOHNSON with multiple cellular devices on the table in front of him. Moreover, in my training and experience, I know that drug traffickers often maintain multiple cellular devices that may be devoted to different aspects of their criminal activity. For example, drug traffickers often have cellular devices devoted to certain customers, a separate device that might be used exclusively for the purpose of contacting drug suppliers, while other devices might be inactive devices that they have maintained because they store customer contact information and other relevant data that has not been transferred to a new device.

30. Moreover, in my training and experience and based on discussions with other members of law enforcement, I understand that iPhones, like SUBJECT DEVICE 3, SUBJECT DEVICE 4 and SUBJECT DEVICE 5, are often linked to Apple laptops like SUBJECT DEVICE 7, for the purpose of backing up, or securing a copy, of the contents of the iPhone. I also understand that SUBJECT DEVICES 1, 2, 3, 4, 5, and 6 are all capable of being used as storage mediums through which digital evidence can be transferred to laptops, like SUBJECT DEVICE 7. Accordingly, there is probable cause to conclude that each of the SUBJECT DEVICES contains evidence of the SUBJECT OFFENSES.

TECHNICAL TERMS

31. As used herein, the following terms have the following meanings:

a) Wireless telephone (or mobile or cellular telephone): A handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving and storing text messages and email; taking, sending, receiving and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device, and a wide variety of applications, also known as "apps," which may store the user's preferences and other data. Such apps may include Facebook, Twitter, and other social media services.

b) "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]"

c) "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); and peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as modems, routers, cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d) "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e) "Hash value" refers to a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated.

f) "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may

include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

g) "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. "Domain name" is a name that identifies an IP address.

h) The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, drives, or electronic notebooks

and tablets, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

29. As described above and in Attachments H-N, this application seeks permission to search for records that would constitute evidence of the SUBJECT OFFENSES. I submit there is probable cause to believe such records will be stored in SUBJECT DEVICES, for at least the following reasons:

a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. *Forensic evidence.* As further described in Attachments H-N, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on SUBJECT DEVICE 7 because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external

storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b) As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally,

some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is

evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

31. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly

likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a

hard drive to human inspection in order to determine whether it is evidence described by the warrant.

33. Based on my research, I understand that the SUBJECT DEVICES provide not only phone and text message services, but can also be used to send and receive emails; access the Internet; track GPS data; take, store and share photographs and videos; and use a wide variety of apps. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the SUBJECT DEVICES.

34. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrants I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrants. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrants.

35. Because this application seeks only permission to examine the SUBJECT DEVICES, which are currently in law enforcement's possession within the Eastern District of New York, the execution of the warrants do not involve intrusion into a physical location. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrants at any time in the day or night.

CONCLUSION

36. Based on the foregoing, there is probable cause to believe that there is located in the SUBJECT DEVICES, further described in Attachments A-G, the things

described in Attachments H-N, which constitute evidence, fruits and instrumentalities of the SUBJECT OFFENSES. Accordingly, the Court should issue the requested warrants.

Special Agent Derek J. Wonderland
Federal Bureau of Investigations
(Sworn by Facetime and/or Telephone Application)

Subscribed and sworn to before me
On [redacted]

HONORABLE ARLENE R. LINDSAY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property To Be Searched

The property to be searched is one gray LG phone with IMEI Number 358335102826284 ("SUBJECT DEVICE 1"), seized on or about November 19, 2020, in Suffolk County, New York. The warrant authorizes the forensic examination of SUBJECT DEVICE 1 for the purpose of identifying the electronically stored information described in Attachment H.

ATTACHMENT B

Property To Be Searched

The property to be searched is one gray LG phone with IMEI Number 354790111345953 ("SUBJECT DEVICE 2"), seized on or about November 19, 2020, in Suffolk County, New York. The warrant authorizes the forensic examination of SUBJECT DEVICE 2 for the purpose of identifying the electronically stored information described in Attachment I.

ATTACHMENT C

Property To Be Searched

The property to be searched is one black iPhone with a white "home button" ("SUBJECT DEVICE 3"), seized on or about November 19, 2020, in Suffolk County, New York. The warrant authorizes the forensic examination of SUBJECT DEVICE 3 for the purpose of identifying the electronically stored information described in Attachment J.

ATTACHMENT D
Property To Be Searched

The property to be searched is one gray iPhone S with Model Number A1688 and FCC ID: BCG-E2946A ("SUBJECT DEVICE 4"); seized on or about November 19, 2020, in Suffolk County, New York. The warrant authorizes the forensic examination of SUBJECT DEVICE 4 for the purpose of identifying the electronically stored information described in Attachment K.

ATTACHMENT E
Property To Be Searched

The property to be searched is one blue iPhone in a clear case ("SUBJECT DEVICE 5"); seized on or about November 19, 2020, in Suffolk County, New York. The warrant authorizes the forensic examination of SUBJECT DEVICE 5 for the purpose of identifying the electronically stored information described in Attachment L.

ATTACHMENT F
Property To Be Searched

The property to be searched is one black LG phone with IMEI Number 356593097595361 and Model Number LML211BL ("SUBJECT DEVICE 6"); seized on or about November 19, 2020, in Suffolk County, New York. The warrant authorizes the forensic examination of SUBJECT DEVICE 6 for the purpose of identifying the electronically stored information described in Attachment M.

ATTACHMENT G
Property To Be Searched

The property to be searched is one gray Apple laptop Model Number A1706 and SN C02TL189GTFJ ("SUBJECT DEVICE 7"); seized on or about November 19, 2020, in Suffolk County, New York. The warrant authorizes the forensic examination of SUBJECT DEVICE 7 for the purpose of identifying the electronically stored information described in Attachment N.

ATTACHMENT H

Particular Things To Be Seized

All information obtained from SUBJECT DEVICE 1 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(b)(1)(A) and 846; and the unlawful possession of a firearm following a felony conviction and in furtherance of a drug trafficking crime in violation of Title 18, United States Code, Sections 922(g) and 924(c), respectively, including:

1. All records and information on SUBJECT DEVICE 1 described in Attachment A, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including IP Addresses, browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

2. Evidence of user attribution showing who used or owned SUBJECT DEVICE 1 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control SUBJECT DEVICE 1, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to SUBJECT DEVICE 1 of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from SUBJECT DEVICE 1;

7. Evidence of the times SUBJECT DEVICE 1 were used;

8. Passwords, encryption keys, and other access devices that may be necessary to access SUBJECT DEVICE 1; and

9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT I

Particular Things To Be Seized

All information obtained from SUBJECT DEVICE 2 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(b)(1)(A) and 846; and the unlawful possession of a firearm following a felony conviction and in furtherance of a drug trafficking crime in violation of Title 18, United States Code, Sections 922(g) and 924(c), respectively, including:

1. All records and information on SUBJECT DEVICE 2 described in Attachment B, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including IP Addresses, browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

2. Evidence of user attribution showing who used or owned SUBJECT DEVICE 2 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control SUBJECT DEVICE 2 such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to SUBJECT DEVICE 2 of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from SUBJECT DEVICE 2;

7. Evidence of the times SUBJECT DEVICE 2 were used;

8. Passwords, encryption keys, and other access devices that may be necessary to access SUBJECT DEVICE 2; and

9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT J

Particular Things To Be Seized

All information obtained from SUBJECT DEVICE 3 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(b)(1)(A) and 846; and the unlawful possession of a firearm following a felony conviction and in furtherance of a drug trafficking crime in violation of Title 18, United States Code, Sections 922(g) and 924(c), respectively, including:

1. All records and information on SUBJECT DEVICE 3 described in Attachment C, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including IP Addresses, browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

2. Evidence of user attribution showing who used or owned SUBJECT DEVICE 3 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control SUBJECT DEVICE 3, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to SUBJECT DEVICE 3 of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from SUBJECT DEVICE 3;

7. Evidence of the times SUBJECT DEVICE 3 were used;

8. Passwords, encryption keys, and other access devices that may be necessary to access SUBJECT DEVICE 3; and

9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT K

Particular Things To Be Seized

All information obtained from SUBJECT DEVICE 4 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(b)(1)(A) and 846; and the unlawful possession of a firearm following a felony conviction and in furtherance of a drug trafficking crime in violation of Title 18, United States Code, Sections 922(g) and 924(c), respectively, including:

1. All records and information on SUBJECT DEVICE 4 described in Attachment D, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including IP Addresses, browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

2. Evidence of user attribution showing who used or owned SUBJECT DEVICE 4 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control SUBJECT DEVICE 4, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to SUBJECT DEVICE 4 of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from SUBJECT DEVICE 4;

7. Evidence of the times SUBJECT DEVICE 4 were used;

8. Passwords, encryption keys, and other access devices that may be necessary to access SUBJECT DEVICE 4; and

9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT L

Particular Things To Be Seized

All information obtained from SUBJECT DEVICE 5 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(b)(1)(A) and 846; and the unlawful possession of a firearm following a felony conviction and in furtherance of a drug trafficking crime in violation of Title 18, United States Code, Sections 922(g) and 924(c), respectively, including:

1. All records and information on SUBJECT DEVICE 5 described in Attachment E, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including IP Addresses, browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

2. Evidence of user attribution showing who used or owned SUBJECT DEVICE 5 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control SUBJECT DEVICE 5, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to SUBJECT DEVICE 5 of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from SUBJECT DEVICE 5;

7. Evidence of the times SUBJECT DEVICE 5 were used;

8. Passwords, encryption keys, and other access devices that may be necessary to access SUBJECT DEVICE 5; and

9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT M

Particular Things To Be Seized

All information obtained from SUBJECT DEVICE 6 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(b)(1)(A) and 846; and the unlawful possession of a firearm following a felony conviction and in furtherance of a drug trafficking crime in violation of Title 18, United States Code, Sections 922(g) and 924(c), respectively, including:

1. All records and information on SUBJECT DEVICE 6 described in Attachment F, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including IP Addresses, browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

2. Evidence of user attribution showing who used or owned SUBJECT DEVICE 6 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control SUBJECT DEVICE 6, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to SUBJECT DEVICE 6 of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from SUBJECT DEVICE 6;

7. Evidence of the times SUBJECT DEVICE 6 were used;

8. Passwords, encryption keys, and other access devices that may be necessary to access SUBJECT DEVICE 6; and

9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT N

Particular Things To Be Seized

All information obtained from SUBJECT DEVICE 7 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(b)(1)(A) and 846; and the unlawful possession of a firearm following a felony conviction and in furtherance of a drug trafficking crime in violation of Title 18, United States Code, Sections 922(g) and 924(c), respectively, including:

1. All records and information on SUBJECT DEVICE 7 described in Attachment G, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including IP Addresses, browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

2. Evidence of user attribution showing who used or owned SUBJECT DEVICE 7 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control SUBJECT DEVICE 7, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to SUBJECT DEVICE 7 of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from SUBJECT DEVICE 7;

7. Evidence of the times SUBJECT DEVICE 7 were used;

8. Passwords, encryption keys, and other access devices that may be necessary to access SUBJECT DEVICE 7; and

9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.